

Remarks

Claims 1-32 are pending. By this Amendment, claims 1, 12, 30 and 31 are amended and new claims 32-33 are added. Reconsideration in view of the above amendments and following remarks is respectfully requested.

Applicant appreciates the courtesies extended by Examiner to Applicant and Applicant's representative during the February 23 personal interview. The points discussed during the interview and incorporated herein.

I. The Claims Define Patentable Subject Matter Pursuant to 35 USC 103

The Office Action rejects claims 1-31 under 35 U.S.C. as being anticipated by U.S. Patent No. 6,519,703 to Joyce (hereinafter "Joyce"). The rejection is respectfully traversed.

The Office Action asserts that Joyce discloses a method for detecting unauthorized intrusion in a network system, including the steps of receiving packet level activity information from the network, sorting port specific activity information from the received packet level activity information, monitoring the port specific activity information, and executing at least one of a blocking action based upon the monitored port specific activity information.

Joyce, however, is directed to a method for analyzing individual packets on a packet by packet basis in a computer network using a heuristic firewall. In Joyce, the packet streams are monitored on a port by port basis. Each packet is judged on an individual basis and packets that are discarded if they are deemed to have low confidence. Thus, the system of Joyce is not

capable of detecting and monitoring various intrusion patterns or detecting new and previously undetected behaviors by separate IP/users.

In contrast, Applicant's invention receives packets which are sorted by IP/user according to port and cross-port behavior. In one embodiment, the system according to the invention converts the network activity to a behavior assessment based upon determinations of expertise (E) and deception (D). The invention then tracks these behavior assessments and blocks certain activity based upon these behavior assessments without regard to the specific packets. In addition, the invention is not a firewall as described in Joyce. Thus, Joyce fails to disclose a behavioral assessment method that is capable of converting the port specific activity information to behavioral assessment measures, monitoring the behavior measures by IP/user and executing at least one of a blocking action or a tracking action based upon the monitored behavior measures, as recited in claim 1. In contrast, Joyce only discards packets that are determined to have low confidence on a packet by packet basis.

Similarly, Joyce fails to disclose a system for preventing unauthorized intrusion in a network system that includes a traffic sorter that receives *a copy* of the network activity and sorts such activity by IP/users; and an activity monitor operatively coupled to the traffic sorter for monitoring converted human behavior measures by IP/users, that is based upon a copy of the network activity, as recited in claim 12. Further, Joyce fails to disclose an inter-port fusion module that fuses assessments from one or more assessment engines that monitor behavior measures, as recited in claim 12.

Thus, Joyce fails to disclose the features of recited in independent claims 1 and 12. It is respectfully submitted that independent claims 30 and 31 are also distinguishable over the applied reference for reasons similar to those described in connection with claim 1 above. Further, dependant claims 2-11 and 13-29 are likewise distinguishable for at least the reasons described above. Therefore, withdrawal of the rejection of claims 1-31 under 35 U.S.C. § 103 is respectfully requested.

CONCLUSION

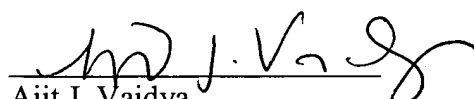
In view of the foregoing, Applicant respectfully requests reconsideration and the allowance of the above-identified application. Should the Examiner feel that there are any issues outstanding after consideration of this response, the Examiner is invited to contact Applicant's representative at the telephone number listed below.

If there are any other fees due in connection with the filing of this response, please charge the fees to our Deposit Account No. 50-1349. If a fee is required for an extension of time under 37 C.F.R. § 1.136 not accounted for above, such an extension is requested and the fee should also be charged to our Deposit Account.

Respectfully submitted,

Dated: March 4, 2005

HOGAN & HARTSON LLP
555 13th Street, N.W.
Washington, D.C. 20004
(202) 637-5600
Customer No. 24633


Ajit J. Vaidya
Registration No. 43,214